CLAIMS

1. A method of electronically identifying and verifying an individual utilising at least one biometric features of the individual including the steps of:

(i) activating an access apparatus with a means to capture at least one biometric feature of an individual in a secure manner using dynamic encryption;

(ii) capturing the biometric feature of an individual wherein key features of biometric raw data are extracted;

(iii) encrypting in a dynamic manner the biometric features;

(iv) transmitting the encrypted data of the biometric feature to at least one server; and

(v) verifying the biometric features captured in step (i) with a pre-stored biometric feature in the server in step (iv).

wherein upon positive identification and verification of the individual access is given to an auxiliary means such as but not limited to access to secured doors, database, computer network and servers.

2. A method of electronically identifying and verifying an individual as claimed in claim 1 wherein the server is either spatially separated from the access apparatus or is contained within the access apparatus.

3. A method electronically identifying and verifying an individual as claimed in claim 1 wherein in step (iv) the encrypted data is transmitted to at least one server in the access apparatus or to at least one server spatially separated from the access apparatus.

4. A method of electronically identifying and verifying an individual as claimed in claim 3 wherein in a first attempt the access apparatus will attempt to send the encrypted data to the spatially separated server.

5. A method of electronically identifying and verifying an individual as claimed in claim 3 wherein upon detecting a failure in the first attempt claim 4 the access apparatus will in a second attempt send the encrypted data to any other designated server in a network.

6. A method of electronically identifying and verifying an individual as claimed in claim 5 wherein the designated servers are either servers spatially separated from the access apparatus or the servers in the access apparatus.

7. A method of electronically identifying and verifying an individual as claimed in claim 1 wherein prior to and independent of step (i) of claim 1 the individual is enrolled into a database by including the steps of:

(i) imputing required particulars of the individual into the database and ascertaining the existence or otherwise of the particulars of the individual in the database;
(ii) capturing the biometric features of the individual wherein key features of the biometric raw data are extracted
(iii) encrypting in a dynamic manner the biometric features, and
(iv) transmitting the encrypted data of the biometric features to the server and storing the encrypted data in relation to the particulars of the individual obtained in step (i) above.

8. A method of electronically identifying and verifying an individual as claimed in claim 1 wherein particulars in step (i) of claim 7 includes alpha-numeral data, and / or images and / or binary data wherein the binary data includes any representation capable of being stored in a binary form.

9. A method of electronically identifying and verifying an individual as claimed in claim 7 wherein at least one spatially separated server is located outside the country.

10. A method of electronically identifying and verifying an individual as claimed in claim 1 wherein the server is provided in a storage medium including a token or other device capable of recording data.

11. A method of electronically identifying and verifying an individual as claimed in claim 1 wherein the identification of the individual is executed by comparing the biometric features of the individual captured in step (ii) of claim 1 with known biometric features of the individual previously captured and stored in a database and picked out from the database by the use of a unique personal identification number (PIN) allocated to the individual and to the records in the database.

12. A method of electronically identifying and verifying an individual as claimed in claim 1 wherein the identification of the individual is executed by comparing the biometric features of the individual captured in step (ii) of claim 1 with known biometric features of the individual previously captured and stored in the database without the use of any PIN numbers.

13. A method of electronically identifying and verifying an individual as claimed in claim 1 wherein the biometric features of the individual to be identified and verified are stored in a server instead of in any storage medium held in possession by or issued to individual.

14. A method of electronically identifying and verifying an individual as claimed in claim 1 wherein the encrypted biometric features of the individual are processed by an biometric server software located at the server instead of at the point where the biometric features of an individual presenting for identification and verification are captured.

15. An electronic means of identifying and verifying an individual presenting for such identification and verification including:

(i) a means to capture at least one type of biometric features of the individual;

(ii) a software means to encrypt in a dynamic manner the biometric features captured in (i);

(iii) a transmission means wherein the encrypted biometric features of the individual is transmitted to a server;

(iv) a software means to capture the encrypted biometric features presented for identification and verification against stored encrypted biometric features of a purported individual; and

(v) a means to give access to other database or software if a positive identification and verification is made and to deny such access if a negative identification and verification is made.

16. An electronic means of identifying and verifying an individual as claimed in claim 15 wherein identifying the individual comprises of:

a PIN number for each stored encrypted biometric features of an individual; and

a means to access the stored encrypted biometric features of an individual by the provision of a correct PIN number by an individual presenting for identification and verification and a means to compare the captured biometric features of the individual with a given PIN number with the stored biometric features of the purported individual.

17. A method of electronically identifying and verifying an individual as claimed in claim 1 wherein the biometric features include finger print, retina scan, iris scan or any other unique biometric features capable of being captured by sensors.

18. An electronic means of identifying and verifying an individual as claimed in claim 15 wherein the biometric features includes finger print, retina scan, iris scan or any other unique biometric feature capable of being captured by sensors.

19. An electronic means of identifying and verifying an individual presenting for such identification and verification including:

(i) access apparatus with a means to capture at least one biometric raw data of an individual in a secure manner using dynamic encryption;

(ii) circuitry to extract any features of the biometric raw data from the means to capture the biometric raw data;

(iii) circuitry to encrypt the key features of the biometric raw data in a dynamic manner;

(iv) transmission means to transmit encrypted data of the biometric features to at least one server;

(v) at least one server to receive and store the encrypted data of the biometric feature of the individual; and

(vi) circuitry to verify and / or identify the encrypted data against pre-stored encrypted biometric data in the server.

20. An electronic means of identifying and verifying an individual as claimed in claim 19 wherein the server is either spatially separated from the access apparatus or is contained within the access apparatus.

21. An electronic means of identifying and verifying an individual as claimed in claim 19 includes circuitry of transmission of encrypted biometric data to a pre-designated server fails, the encrypted biometric data is routable to at least one other designated server in an pre-designated sequence.

22. An electronic means of identifying and verifying an individual as claimed in claim 1 wherein a token encoding data unique to the individual presenting for identification and verification has to be introduced into the access apparatus before the biometric feature of the individual is captured.

23. An electronic means of identifying and verifying an individual as claimed in claim 1 wherein the biometric data of an individual is stored in a encrypted manner in server and in any tokens if used.

24. An electronic means of identifying and verifying an individual as claimed in claim 1 wherein the means requires the introduction of a personal identification number (PIN) of an individual presenting for identification and verification into the access apparatus.